REMARKS/ARGUMENTS

Twenty-three claims were pending in this application. In the above amendment, seven claims (3, 4, 15, 19, and 21-23) were cancelled, and twelve claims (1, 5-12, 14, 18, and 20) were amended. Accordingly, sixteen claims (1, 2, 5 – 14, 16 – 18, and 20) remain pending. This amendment adds no new matter.

Applicants respectfully traverse the rejections over the Hurtado reference (2003/0105718). Applicants readily admit that the use of digital certificates and encryption keys is well known – the Hurtado reference plainly discloses that. However, Applicants have provided a storage-engine-based authentication procedure that provided enhanced security with respect to conventional DRM schemes such as that disclosed in the Hurtado reference. For example, as discussed with respect to the authentication procedure of Figure 6 on page 29, line 13 through page 30, line 2, a host device 606 seeking to gain access to content on media 602 provides a certificate to storage engine 604. After verifying digital signatures on the certificate and validating the host (checking for revocation), the storage engine generates a random number (the secure session key) that is then encrypted according to a public key on the certificate. The host may then recover the secure session key using the corresponding private key.

Content on the media is encrypted according to a content key. Thus, the host needs the content key to gain access to the content. However, for additional security, the storage engine does not simply provide the content key to the host. Instead, the content key is encrypted using the secure session key. Thus, the host can only recover the content key using the secure session key. As such, the secure session key is not a content key but rather is a key to the content key.

Claim 1 has been amended to more particularly point out and distinctly claim the invention described above. For example, claim 1 now recites the limitations of "if the digital signatures are verified and validated, generating a random number at the storage engine and encrypting the random number with a public key extracted from the certificate to form a session key and transmitting the session key to the host; at the host, receiving an encrypted content key from the storage engine; and decrypting the encrypted content key using the session key to recover the content key.

Hurtado makes no teaching or suggestion for such a secure DRM technique. Accordingly, claim 1 and its dependent claims 2, 5-14, and 16-18 are allowable.

Claim 20 has been amended analogously as discussed with respect to claim 1. Accordingly, claim 20 is also allowable over the Hurtado reference.

CONCLUSION

For the above reasons, claims 1, 2, 5 – 14, 16 – 18, and 20 are now in a condition for allowance. Applicant therefore respectfully requests that a timely Notice of Allowance be issued in this case.

If there are any questions regarding this amendment, the Examiner is invited to call the undersigned at (949) 752-7040.

Certification of Facsimile Transmission
I hereby certify that this paper is being facsimile transmitted to the U.S. Patent and Trademark Office on the date shown below.

Jonathan Hallman — February 16, 2005
Jonathan Hallman — Date of Signature

Respectfully submitted,

Jonathan W. Hallman
Attorney for Applicants
Reg. No. 42,622
Tel.: (949) 752-7040